

# A Tight Lower Bound for the BB84-states Quantum-Position-Verification Protocol

Jérémy Ribeiro and Frédéric Grosshans\*

Laboratoire Aimé Cotton, CNRS, Université Paris-Sud and ENS Cachan, F-91405 Orsay, France

We use the entanglement sampling techniques developed by Dupuis, Fawzi and Wehner [1] to find a lower bound on the entanglement needed by a coalition of cheaters attacking the quantum position verification protocol using the four BB84 states [2, 3] ( $\text{QPV}_{\text{BB84}}$ ) in the scenario where the cheaters have no access to a quantum channel but share a (possibly mixed) entangled state  $\tilde{\Phi}$ . For a protocol using  $n$  qubits, a necessary condition for cheating is that the max- relative entropy of entanglement  $E_{\max}(\tilde{\Phi}) \geq n - O(\log n)$ . This improves previously known best lower bound by a factor  $\sim 4$ , and it is essentially tight, since it is vulnerable to a teleportation based attack using  $n - O(1)$  ebits of entanglement.

PACS numbers: 03.67.Dd, 03.67.Mn, 89.70.Cf

The very first (classical) position verification (PV) protocols have been distance bounding protocols, introduced in 1993 [4] to prevent man-in-the-middle attacks. Based on the speed-limit  $c$  on information propagation imposed by special relativity, they can only work when the prover  $P$  and the verifier  $V$  are close, and are useless against nearby malicious adversaries  $M$ , *i.e.* when  $\text{distance}(M, V) \leq \text{distance}(P, V)$  [5]. PV protocols by a coalition of distant verifiers  $\{V_i\}$  are therefore needed in such situation, as they allow to build localized authentication protocol, but also many other cryptographic applications, like key distribution at a specific place [6]. However, Chandran *et al.* have shown in 2009 [6] that no classical PV protocol can be computationally secure against a coalition  $\{M_i\}$  of malicious provers. They only found a protocol secure in the bounded retrieval model.

Quantum position verification (QPV) protocols appeared the next year in the scientific literature, with publications of three independent teams [2, 3, 7–10]. Even in the quantum case, unconditional security is unattainable [3], and a universal attack using an exponential amount of entanglement as been found by Beigi and König [11]. To guarantee the security of a QPV protocol one either need a computational hypothesis [12] or a bound on the quantum entanglement shared between the cheaters [3, 11, 13, 14].

The present work is in the latter framework, where the cheating coalition  $\{M_i\}$  only has access to a limited amount of entanglement. Despite the exponential universal attack [11], all lower bounds found so far have been linear [11, 14] or sub-linear [3, 13]. To our knowledge, the protocol showing the best security in this framework is the protocol using mutually unbiased bases  $\text{QPV}_{\text{MUBs}}$  proposed by Beigi and König in [11]. A  $n$ -qubits implementation of  $\text{QPV}_{\text{MUBs}}$  is secure against adversary holding less than  $n/2$  ebits. However,  $\text{QPV}_{\text{MUBs}}$  needs the coherent manipulation of  $n$  qubits and is therefore impossible to implement with present day technologies.

$\text{QPV}_{\text{BB84}}$ , introduced in [2, 3] and defined below, is experimentally much simpler since it essentially uses quantum key distribution components [15, 16], and Tomamichel *et al.* [14] have proved its security against adversary holding less than  $-\log_2(\cos^2(\pi/8)) \cdot n \simeq 0.22845 \cdot n$  ebits of entanglement. We improve this bound to  $n - O(\log n)$  ebits. Since a teleportation-based explicit attack using  $n - O(1)$  ebits is

known [8, 13], this bound is tight.

We start this letter by giving some useful properties of the min-entropy  $H_{\min}$  and the max- relative entropy of entanglement  $E_{\max}$ , a related entanglement monotone. Since our security proof is based on an adaptation of the entanglement sampling based security proof [1] of weak string erasure (WSE) in the noisy storage model (NSM), we then describe this protocol. We then show its security the noisy entanglement model (NEM) and use it to show the security of  $\text{QPV}_{\text{BB84}}$ .

In the following  $\mathcal{S}(A)$  is the set of quantum states of the system  $A$ .

**Definition 1** (min-entropy). *Let  $\varrho \in \mathcal{S}(AB)$  be a bipartite state. The conditional min-entropy  $H_{\min}(A|B)_{\varrho}$  is*

$$H_{\min}(A|B)_{\varrho} := - \inf_{\tau \in \mathcal{S}(B)} \inf \{ \lambda \in \mathbb{R} : \varrho \leq 2^{\lambda} \mathbb{I}_A \otimes \tau \}$$

The following property shows the conditional min-entropy of a classical-quantum ( $cq$ ) state is essentially the logarithm of the probability to guess the classical part from the quantum part.

**Property 2.** [17, theorem 1] *Let  $\varrho \in \mathcal{S}(XB)$  be a  $cq$ -state, *i.e.* a state of the form  $\varrho = \sum_x p_x |x\rangle\langle x| \otimes \tau_x$  with  $\tau_x \in \mathcal{S}(B) \forall x$ . Then,*

$$H_{\min}(X|B)_{\varrho} = -\log_2 p_{\text{guess}}(X|B)_{\varrho},$$

where  $p_{\text{guess}}(X|B)_{\varrho}$  is the maximal probability of guessing the value of  $X$  from an optimal measurement on  $B$ .

The max- relative entropy of entanglement has been introduced by Datta [18] as an entanglement monotone closely related to  $H_{\min}$ .

**Definition 3** (max- relative entropy of entanglement). *Let  $\varrho \in \mathcal{S}(AB)$  be a bipartite state. Its max- relative entropy of entanglement is noted  $E_{\max}(\varrho)_{A;B}$  or  $E_{\max}(A; B)_{\varrho}$  and is*

$$E_{\max}(A; B)_{\varrho} := \inf_{\sigma \in \mathcal{D}} \inf \{ \lambda \in \mathbb{R} : \varrho \leq 2^{\lambda} \sigma \}$$

where  $\mathcal{D}$  is the set of separable states of  $\mathcal{S}(AB)$ .

**Property 4** (monotony of  $E_{\max}$ ). [18, theorem 1] *The max-relative entropy of entanglement  $E_{\max}$  is an entanglement monotone, i.e. it can only decrease under local operations and classical communications (LOCC). More formally, let  $\Lambda$  be completely positive trace preserving (CPTP) map  $\mathcal{S}(AB) \rightarrow \mathcal{S}(A'B')$  which can be achieved through LOCCs.*

$$E_{\max}(\varrho)_{A;B} \geq E_{\max}(\Lambda(\varrho))_{A';B'}$$

In order to establish the theorem 6 linking  $E_{\max}$  and  $H_{\min}$ , we will need the following lemma :

**Lemma 5.** *Let  $\mathcal{D}(A:B) \subset \mathcal{S}(A, B)$  be the set of separable states, i.e. the convex hull of the set of product states  $\mathcal{S}(A) \otimes \mathcal{S}(B)$ . For any state  $\sigma \in \mathcal{D}(A:B)$ , there exists a state  $\tau \in \mathcal{S}(B)$  such that  $\sigma \leq \mathbb{I} \otimes \tau$ .*

*Proof.* Let  $\sigma \in \mathcal{D}(A; B)$ , there exists a mixture  $\{p_i, \tau_A^i \otimes \tau_B^i\}_i$  of states of  $\mathcal{S}(A) \otimes \mathcal{S}(B)$  such that

$$\begin{aligned} \sigma &= \sum_i p_i \tau_A^i \otimes \tau_B^i && \text{since } \sigma \in \mathcal{D}(A:B) \\ &\leq \sum_i p_i \mathbb{I}_A \otimes \tau_B^i && \text{since } \forall i, \tau_A^i \leq \mathbb{I}_A \\ &= \mathbb{I}_A \otimes \sum_i p_i \tau_B^i = \mathbb{I}_A \otimes \tau && \text{defining } \tau := \sum_i p_i \tau_B^i \end{aligned}$$

□

**Theorem 6.** *For any bipartite state  $\varrho \in \mathcal{S}(AB)$ ,*

$$E_{\max}(A; B)_{\varrho} \geq -H_{\min}(A|B)_{\varrho}$$

*Proof.* For any separable state  $\sigma \in \mathcal{D}(A : B)$ , there exists a state  $\tau \in \mathcal{S}(B)$  such that

$$\begin{aligned} \varrho &\leq 2^{E_{\max}(A;B)_{\varrho}} \sigma && \text{(from definition 3)} \\ &\leq 2^{E_{\max}(A;B)_{\varrho}} \mathbb{I}_A \otimes \tau && \text{(lemma 5)} \end{aligned}$$

The definition of  $-H_{\min}$  as lower bound (definition 1) then implies  $H_{\min}(A|B)_{\varrho} \leq -E_{\max}(A; B)_{\varrho}$ . □

Now that we have the relevant properties of  $H_{\min}$  and  $E_{\max}$ , we study the weak string erasure (WSE) protocol. It was introduced, together with the noisy storage model (NSM) by König *et al.* [19] to build secure bipartite protocols. The NSM is based on a technological limit imposed on quantum memories : after a delay  $\Delta t$ , the quantum state they can hold decoheres and becomes noisy. In this model, a protocol is split in two phases. A bipartite protocol involving the traditionally named Alice (A) and Bob (B) can therefore be seen as a quadripartite protocol between two coalitions : it first involves early-Alice ( $A_1$ ) and early-Bob ( $B_1$ ), and then, after  $\Delta t$ , later-Alice ( $A_2$ ) and later-Bob ( $B_2$ ). A noisy quantum memory held by Bob is then modeled by a noisy quantum channel  $\mathbb{F} : B_1 \rightarrow B_2$ .

The WSE protocol proposed in [19] can be described as follows, for honest Alice(s) and Bob(s):

1.  $A_1$  choses uniformly at random  $X^n = \{x_i\}_i$  and  $\Theta^n = \{\vartheta_i\}_i$ , two bit strings of length  $n$ .
2.  $B_1$  choses uniformly at random  $\tilde{\Theta}^n = \{\tilde{\vartheta}_i\}_i$ , a bit string of length  $n$ .
3.  $A_1$  sends to  $B_1$  the quantum state  $\bigotimes_i \hat{H}^{\vartheta_i} |x_i\rangle$ , where  $\hat{H}$  is the Hadamard operator and  $\{|0\rangle, |1\rangle\}$  the computational basis of a qubit. It is the BB84 encoding of the string  $X^n$  in the basis  $\Theta^n$ .
4.  $B_1$  measures the qubits in the bases  $\tilde{\Theta}^n$ , and gets the string  $\tilde{X}^n$ .
5. Both parties wait the time  $\Delta t$ . The classical memories of Alice and Bob corresponds to classical channels allowing  $A_1$  to send  $\{X^n, \Theta^n\}$  to  $A_2$  and  $B_1$  to send  $\{\tilde{X}^n, \tilde{\Theta}^n\}$  to  $B_2$ .
6.  $A_2$  sends  $\Theta^n$  to  $B_2$ .
7.  $B_2$  computes  $I = \{i : \vartheta_i = \tilde{\vartheta}_i\}$  and  $\tilde{X}^I = X^I$

We are interested here by the correctness of the protocol, but only by its security against a dishonest Bob.

**Definition 7.** *A WSE protocol is  $\lambda$ -secure against Bob if the probability for  $B_2$  to correctly guess the string  $X^n$  is smaller than  $2^{-n\lambda}$ . More formally, let  $\mathcal{C}(A_2, B_2)$  be the set of all possible states  $\sigma_{A_2, B_2}$  which can be obtained at the end of the protocol if Alice follows it but Bob is dishonest. The protocol is secure for Alice if,  $\forall \sigma \in \mathcal{C}(A_2, B_2)$ ,*

$$\frac{1}{n} H_{\min}(X^n | B_2)_{\sigma} \geq \lambda.$$

Instead of the  $\lambda$ -security, which ensures exponential security with  $n$  as long as  $\lambda > 0$ , one can also be interested in the  $\varepsilon$ -security for a fixed  $n$  :

**Definition 8.** *A protocol is  $\varepsilon$ -secure iff, for any possible dishonest strategy, the probability  $p_{\text{cheat}}$  for a dishonest adversary to win is  $p_{\text{cheat}} < \varepsilon$ .*

**Lemma 9.** *For a protocol like WSE or QPV<sub>BB84</sub>, where the goal of the cheater is to guess a classical string  $X^n$ ,  $\lambda$ -security and  $\varepsilon$ -security are equivalent notions when*

$$\varepsilon = 2^{-n\lambda} \Leftrightarrow \lambda = -\frac{1}{n} \log_2 \varepsilon$$

*Proof.* This follows directly from the definitions and property 2. □

In the NSM model, a dishonest Bob changes the above protocol in the following way:

4.  $B_1$  performs a generalized measurement on the qubits, obtaining a joint  $cq$ -system  $CQ_1$ .
5. During the  $\Delta t$  wait,  $B_1$  stores this state in his memory. While the classical memory is perfect, the quantum memory is described by the noisy channel  $\mathbb{F}$ , and  $B_2$  obtains  $CQ_2 = (\mathbb{I} \otimes \mathbb{F})(CQ_1)$ .

7. At the final step, the global quantum state is  $\sigma \in \mathcal{S}(X^n \Theta^n C Q_2)$ , where  $A_2$  holds the classical information  $X^n$  and  $B_2$  has access to the classical information  $\Theta^n C$ , as well as to the quantum information  $Q_2$ .  $B_2$  tries to guess  $X^n$  from  $\Theta^n C Q_2$  and the security of the protocol is measured by  $H_{\min}(X^n | \Theta^n C Q_2)_\sigma$ .

**Theorem 10.** ([1, theorem 14]) *Let Bob storage device  $\mathbb{F}$  have a maximal fidelity, as defined in [1], upper bounded by  $\eta$ . The WSE protocol defined above is  $\lambda$ -secure for*

$$\lambda \leq \frac{1}{2} \left[ \gamma \left( -1 - \frac{1}{n} \log_2 \eta \right) - \frac{1}{n} \right],$$

where  $\gamma$  is the function defined by

$$\gamma(h_{\min}) := \begin{cases} h_{\min} & \text{if } h_{\min} \geq \frac{1}{2} \\ g^{-1}(h_{\min}) & \text{if } h_{\min} < \frac{1}{2}, \end{cases}$$

$g(\alpha) := h(\alpha) + \alpha - 1$ ;  $h(\alpha) := -\alpha \log_2 \alpha - (1 - \alpha) \log_2 (1 - \alpha)$  is the binary entropy function.

We defer the reader to [1] for the proof of this theorem. We will now reformulate it in a slightly different security model, the noisy entanglement model (NEM).

In the NEM,  $A_1$ ,  $A_2$ ,  $B_1$  and  $B_2$  are actually four different persons, localized at different places and connected with (unlimited) classical channels  $A_1 \rightarrow A_2$  and  $B_1 \rightarrow B_2$ . The protocol WSE is the same as described above, except that there is no specific  $\Delta t$  at the step 5.  $B_1$  and  $B_2$  also share a (possibly mixed) entangled state  $\tilde{\Phi}_{Q_1, Q_2}$  instead of a quantum channel  $\mathbb{F}$ . The two models are obviously related, since one can create a state  $\tilde{\Phi}$  by transmitting it through  $\mathbb{F}$ , and one can create a channel  $\mathbb{F}$  through teleportation, using  $\tilde{\Phi}$  and the unlimited classical channel.

We now adapt theorem 10 to NEM, exactly following Dupuis *et al.*'s proof [1] until their corollary 11 and slightly changing it after. As usual, we study the equivalent entangled protocol, where  $A_1$  prepares a maximally entangled state  $|\Phi^+\rangle_{AA'}^{\otimes n}$ , sends the  $A'^n$  half to  $B_1$  and gives the  $A^n$  half to  $A_2$ .  $A_2$  finds the string  $X^n$  by measuring  $A^n$  in the basis  $\Theta^n$ .

**Lemma 11.** [1, corollary 11] *With the notations above, and  $\gamma$  defined in theorem 10, we have*

$$H_{\min}(X^n | \Theta^n C Q_2)_\sigma \geq \frac{1}{2} \left[ n \gamma \left( \frac{1}{n} H_{\min}(A^n | C Q_2)_\sigma \right) - 1 \right]$$

We can now show the security of WSE in NEM :

**Theorem 12.** *Let the dishonest Bobs share a (possibly mixed) entangled state  $\tilde{\Phi} \in \mathcal{S}(B_1, B_2)$ . In the NEM, the WSE protocol defined above is  $\lambda$ -secure if*

$$\lambda \leq \frac{1}{2} \left[ \gamma \left( -\frac{1}{n} E_{\max}(\tilde{\Phi}) \right) - \frac{1}{n} \right]$$

*Proof.* We will look at the entanglement between  $B_2$  and the other partners  $A_1 A_2 B_1$ . The only entanglement which exists at the beginning of the protocol comes from  $\tilde{\Phi}$ . Then all the

operations specified by the protocol, as well as the ones allowed in the NEM, are LOCCs according to the  $A_1 A_2 B_1 : B_2$  split. We have therefore

$$\begin{aligned} -E_{\max}(\tilde{\Phi}) &\leq -E_{\max}(\sigma)_{A^n; C Q_2} && \text{(property 4)} \\ &\leq H_{\min}(A^n | C Q_2)_\sigma && \text{(theorem 6),} \end{aligned}$$

where  $\sigma$  denotes the state shared by  $A_2$  and  $B_2$  just before their measurements.

Applying the monotonously increasing function  $\gamma$  leads us to

$$\gamma \left( -\frac{1}{n} E_{\max}(\tilde{\Phi}) \right) \leq \gamma \left( \frac{1}{n} H_{\min}(A^n | C Q_2)_\sigma \right)$$

Lemma 11 then gives

$$\leq \frac{2}{n} H_{\min}(X^n | \Theta^n C Q_2) + \frac{1}{n},$$

which with some reordering and the definition 7 of  $\lambda$  concludes the proof.  $\square$

**Corollary 13.** *Let  $\varepsilon > 0$ . WSE is  $\varepsilon$ -secure in the NEM if*

$$E_{\max}(\tilde{\Phi}) \leq n - s - n h \left( \frac{s}{n} \right)$$

where  $s := 1 - 2 \log_2 \varepsilon$  and  $e$  is the basis of the natural logarithm. A slightly more stringent sufficient condition is :

$$E_{\max}(\tilde{\Phi}) \leq n - s \log_2 n + s \log_2 \frac{s}{2e}$$

*Proof.* According to theorem 12, the protocol is  $\lambda$ -secure for

$$\begin{aligned} \frac{1}{2} \left[ \gamma \left( -\frac{1}{n} E_{\max}(\tilde{\Phi}) \right) - \frac{1}{n} \right] &\geq \lambda \\ \gamma \left( -\frac{1}{n} E_{\max}(\tilde{\Phi}) \right) &\geq \frac{1}{n} + 2\lambda \\ &= \frac{1}{n} - \frac{2}{n} \log_2 \varepsilon \quad (\text{lemma 9}) \\ &=: \frac{s}{n} \end{aligned}$$

applying  $g = \gamma^{-1}$  to both sides leads to

$$\begin{aligned} -\frac{1}{n} E_{\max}(\tilde{\Phi}) &\geq g \left( \frac{s}{n} \right) \\ E_{\max}(\tilde{\Phi}) &\leq -n g \left( \frac{s}{n} \right) = n - s - n h \left( \frac{s}{n} \right) \end{aligned}$$

which gives the first inequality of the theorem.

A straightforward study of the binary entropy functions shows that  $n h \left( \frac{s}{n} \right) \leq s \log_2 n - s \log_2 \frac{s}{e}$ . Substituting this expression in the above equation concludes the proof.  $\square$

We have now all the elements to prove the security of a QPV protocol. For the sake of simplicity, we limit ourselves to the unidimensional case. In this case a QPV protocol involves two verifiers  $\{V_1, V_2\}$  and a prover P between them. The QPV<sub>BB84</sub> protocol [3] can be described as follows

1.  $V_1$  and  $V_2$  privately chose the strings  $X^n$  and  $\Theta^n$ .
2.  $V_1$  sends to P the quantum state  $\bigotimes_i \hat{H}^{\vartheta_i} |x_i\rangle$ .

3.  $V_2$  sends  $\Theta^n$  to P.
4. P receives the messages of  $\{V_1, V_2\}$  simultaneously. He measures the qubits in the base  $\Theta^n$  and obtains  $\tilde{X}^n = X^n$ . He immediately broadcasts  $\tilde{X}^n$  to  $\{V_1, V_2\}$ .
5.  $\{V_1, V_2\}$  accept P's position iff  $\tilde{X}^n = X^n$  and if they receive this information on time

The timing is such that P has to be at the right place to receive both the qubits and  $\Theta^n$ , and then broadcast the measurement result to  $V_1$  and  $V_2$  on time. We refer the reader to [3] for a precise definition of the timing and the correctness condition, as we are mainly concerned by the cheating strategies.

We now study the security of this protocol against a coalition of two malicious cheaters  $\{M_1, M_2\}$ ,  $M_1$  (resp.  $M_2$ ) being closer to  $V_1$  (resp.  $V_2$ ) than P is supposed to be. The timing constraints allow them a single round of classical communications. In the NEM they have access to no quantum communications, except an initially shared bipartite state  $\tilde{\Phi} \in \mathcal{S}(M_1, M_2)$ . Note that an access to a quantum information channel of finite entanglement cost [20] can be brought in this model through the corresponding state  $\Phi$ . The possible action of the cheaters are:

1.  $M_1$  performs a generalized measurement on the qubits sent by  $V_1$  and his half  $M_1$  of the state  $\Phi$ . He gets a classical quantum system  $C_1 Q_1$  and sends  $C_1$  to  $M_2$
2. Depending on  $\Theta^n$ ,  $M_2$  performs a generalized measurement on his half  $M_2$  of the state  $\Phi$ . He obtains a  $C_2 Q_2$  and sends  $C_2$  to  $M_1$
3. Receiving  $C_{i\pm 1}$ ,  $M_i$  extracts his best guess  $X_i^n$  from  $C_1 C_2 Q_i$  and sends it to  $V_i$

This looks like an attack on WSE in the NEM, where  $\{V_i\}_i = \{A_i\}_i$  and  $\{M_i\}_i = \{B_i\}_i$ , with the supplementary requirement that  $M_1 = B_1$  has also to output  $X^n$ . In particular, it means that any attack on QPV<sub>BB84</sub> leads to an attack on QPV<sub>BB84</sub> in NEM, leading us to our main result :

**Theorem 14.** QPV<sub>BB84</sub> is  $\varepsilon$ -secure if the state  $\Phi$  shared by  $M_1$  and  $M_2$  verifies

$$E_{\max}(\tilde{\Phi}) \leq n - s - nh\left(\frac{s}{n}\right)$$

where  $s := 1 - 2 \log_2 \varepsilon$  and  $e$  is the basis of the natural logarithm. A slightly more stringent sufficient condition is :

$$E_{\max}(\tilde{\Phi}) \leq n - s \log_2 n + s \log_2 \frac{s}{2e}$$

*Proof.* Corollary 13 ensures that WSE is  $\varepsilon$ -secure in the NEM against adversaries using  $\Phi$  as resource. We will now prove by contradiction that QPV<sub>BB84</sub> is also  $\varepsilon$ -secure.

Let us suppose it is not the case:  $M_1$  and  $M_2$  have a cheating strategy winning in QPV<sub>BB84</sub> with probability  $P_{\text{cheat}}^{\text{QPV}} > \varepsilon$ . They can use this strategy as  $B_1$  and  $B_2$  in a WSE protocol, without the  $M_2 \rightarrow M_1$  communication and the final broadcasts of  $X_i^n$ ,

and using  $X_2^n$  as guess for  $X^n$ . Their probability to cheat WSE is  $P_{\text{cheat}}^{\text{WSE}} = P(X_2^n = X^n) \geq P_{\text{cheat}}^{\text{QPV}} > \varepsilon$ : WSE is not  $\varepsilon$ -secure, which is contradictory with corollary 13.

Therefore, QPV<sub>BB84</sub> is  $\varepsilon$ -secure.  $\square$

We have shown the security of the practical protocol QPV<sub>BB84</sub> in one dimension against a coalition of cheaters sharing an entangled state of max- relative entropy of entanglement  $E_{\max}(\Phi) \leq n - O(\log n)$ . This bound is the best known to date for a QPV protocol and is essentially tight for QPV<sub>BB84</sub>, since an attack using  $n - O(1)$  ebits is known [8, 13]. While this method probably generalizes to the multidimensional case using tools from [12], as well as to other protocols, like QPV<sub>MUBs</sub> [11] and non-Pauli variants of QPV<sub>BB84</sub> [8, 13], it will not approach the exponential upper bound of these protocols. This method is also useless when  $M_1$  and  $M_2$  have access to an unlimited quantum channel (but did not use it for some reason to share entanglement before the protocol starts), while the bound of [14] works in this case.

We thank Christian Schaffner, Anthony Leverrier, Kaushik Chakraborty, Omar Fawzi and Jędrzej Kaniewski for stimulating discussions. FG specially thanks Christian Schaffner for introducing him to position based cryptography, and for maintaining the webpage [21], a precious resource to begin in this domain.

---

\* frederic.grosshans@u-psud.fr

- [1] F. Dupuis, O. Fawzi, and S. Wehner, IEEE Transactions on Information Theory **61**, 1093 (2015), arXiv:1305.1316.
- [2] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky, (2010), withdrawn and replaced by [3], arXiv:1005.1750v1.
- [3] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, SIAM Journal on Computing **43**, 150 (2014), arXiv:1009.2490.
- [4] S. Brands and D. Chaum, in *Advances in Cryptology — EUROCRYPT '93*, Lecture Notes in Computer Science, Vol. 765, edited by T. Hellesest (Springer Berlin Heidelberg, 1994) pp. 344–359.
- [5] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, J. Comput. Secur. **19**, 289 (2011).
- [6] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, in *Advances in Cryptology - CRYPTO 2009*, Lecture Notes in Computer Science, Vol. 5677, edited by S. Halevi (Springer Berlin Heidelberg, 2009) pp. 391–407, IACR:2009/364.
- [7] A. P. Kent, W. J. Munro, T. P. Spiller, and R. G. Beausoleil, “Quantum tagging,” US patent 7,075,438 (2006).
- [8] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011), arXiv:1008.2147.
- [9] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010), arXiv:1003.0949.
- [10] R. A. Malaney, in *Global Telecommunications Conference (GLOBECOM 2010)*, 2010 IEEE (2010) pp. 1–6, arXiv:1004.4689.
- [11] S. Beigi and R. König, New Journal of Physics **13**, 093036 (2011), arXiv:1101.1065.
- [12] D. Unruh, in *Advances in Cryptology – CRYPTO 2014*, Lecture Notes in Computer Science, Vol. 8617, edited by J. A. Garay

- and R. Gennaro (Springer Berlin Heidelberg, 2014) pp. 1–18, IACR:2014/118.
- [13] H.-K. Lau and H.-K. Lo, Phys. Rev. A **83**, 012322 (2011), arXiv:1009.2256.
  - [14] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, New Journal of Physics **15**, 103002 (2013), arXiv:1210.4359.
  - [15] C. H. Bennett and G. Brassard, in *IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (Bangalore, India, 1984) p. 8.
  - [16] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009), arXiv:0802.4155.
  - [17] R. König, R. Renner, and C. Schaffner, IEEE Transactions on Information Theory **55**, 4337 (2009), arXiv:0807.1338.
  - [18] N. Datta, Information Theory, IEEE Transactions on **55**, 2816 (2009), arXiv:0803.2770.
  - [19] R. König, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012), arXiv:0906.1030.
  - [20] M. Berta, F. G. Brandão, M. Christandl, and S. Wehner, IEEE Transactions on Information Theory **59**, 6779 (2013), arXiv:1108.5357.
  - [21] C. Schaffner, “Personal homepage of Christian Schaffner / position based quantum crypto,” <http://homepages.cwi.nl/~schaffne/positionbasedqcrypto.php> (2015).